



Random Number Generator Evaluation Report

13 January 2009



1. Operator

Casino770.com, 770.com	URL: www.casino770.com
Casino Riva	URL: www.casinoriva.com
To: John	e-mail: (john@casino770.com)
CC:	e-mail: (technique@casino770.com)

2. Test house

iTech Labs Australia	URL: http://www.itechlabs.com.au
Suite 24, 40 Montclair Ave Glen Waverley VIC 3150, Australia	e-mail: info@itechlabs.com.au

3. Software Provider

Fast Cpu	URL: www.fast-cpu.com
Address: FLAT 1, 26 CLEVELAND ROAD, SOUTH WOODFORD, LONDON, E182AN	
To: John	e-mail: (john@casino770.com)
CC:	e-mail: (technique@casino770.com)

4. System/Module tested

System: N/A	URL: N/A
Module: Random Number Generator (RNG) using Mersenne Twister algorithm.	
Date Completed: 1 January 2009	

5. Previous history of items under test

None.

6. Evaluation performed

iTech Labs has conducted evaluation for the RNG implementation using Mersenne Twister algorithm as below:

<p>This RNG consisted of implementation of Mersenne Twister algorithm. Our evaluation of the RNG consisted of source code evaluation, Diehard tests on the raw numbers generated by the algorithm and Chi-square tests on the shuffled decks for card games and various ranges for non-card games.</p> <ol style="list-style-type: none">1. Source code examination The following source code evaluation was conducted:<ol style="list-style-type: none">a) Identification of RNG algorithm;
--

- b) Security of internal state, seeding and re-seeding, thread safety;
- c) Shuffling of cards;
- d) Scaling for the ranges required for the non-card games

2. Tests conducted

- a) Marsaglia's "Diehard" tests were applied to 80 million bits of raw 32 bit random numbers generated by the Mersenne Twister algorithm. The following diehard tests were conducted on 2 sets of 80 million bits;

- i) BIRTHDAY SPACINGS
- ii) OVERLAPPING 5-PERMUTATIONS
- iii) BINARY RANK TEST for 31x31 matrices
- iv) BINARY RANK TEST for 32x32 matrices
- v) BINARY RANK TEST for 6x8 matrices
- vi) BITSTREAM TESTS ON 20-BIT Words
- vii) BITSTREAM TESTS OPSO, OQSO, DNA
- viii) COUNT-THE-1's IN A STREAM OF BYTES
- ix) COUNT-THE-1's IN SPECIFIC BYTES
- x) PARKING LOT TEST
- xi) MINIMUM DISTANCE TEST
- xii) THE 3DSPHERES TEST
- xiii) THE SQUEEZE test
- xiv) OVERLAPPING SUMS TEST
- xv) RUNS TEST
- xvi) CRAPS TEST

- b) The following Chi-squared tests were conducted:

- i) Shuffling tests for 1 (without a joker and with 1 and 2 jokers), 4, 6 and 8 decks of cards. These tests were conducted using samples ranging from 1,000 to 100,000 deals for a total of over 2.5 million deals
- ii) Scaling tests for the ranges 2, 3, 4, 5, 7, 8, 9, 15, 16, 17, 24, 31, 32, 33, 37, 38, 43, 48, 63, 64, 65, 66, 68, 71, 110, 127, 128, 129, 151, 171, 196, 197, 200, 210, 232, 233, 241, 255, 256, 257, 280, 300, 331, 350, 363, 371, 376, 437, 441, 450.

The RNG tests were conducted for compliance to relevant Alderney Gambling Control Commission (AGCC), UK Gambling Commission, Isle of Man and Malta standards.

7. Evaluation results:

1. Source code examination

Fast Cpu RNG implements Mersenne Twister (MT) algorithm.

We identified one issue regarding scaling. This was resolved in the updated code provided by Fast Cpu.

The RNG state is initialised from an entropy source. As per the reviewed source code the RNG is not reseeded. The internal state of the Fast Cpu RNG is thread-safe.

2. Tests conducted

- a) Marsaglia's "Diehard" tests
The results were satisfactory.
- b) Chi-squared tests
 - i) Shuffling tests
The results were satisfactory.
 - ii) Scaling tests for the specified ranges



The results were satisfactory.

8. Observations

1. The internal state of the RNG module can be accessed through the client/server interface* by another program running on the server, but the visible output is encrypted with SHA256. Since deriving the value from a SHA digest is considered an extremely difficult task mathematically, the computation of the internal state of the RNG by another program is virtually impossible for all practical purposes.

* Note: In the Client/Server architecture employed for this RNG implementation, the RNG server implements the algorithm and the game clients request raw 32 bit random numbers from the server.

9. Certification

Date of Certification: 13 January 2009
Software provider: Fast Cpu
Operator: Casino770.com, 770.com, Casino Riva
Total number of pages: 5

iTech Labs certifies that the RNG (listed in Appendix-A) comply with Alderney Gambling Control Commission (AGCC), UK Gambling Commission, Isle of Man and Malta standards subject to the conditions in *section 10 Conditions*.

10. Conditions of Certification

1. The source code provided to iTech Labs (as per Appendix-A) must be used for compilation of the RNG module.
3. Any change to the RNG source files listed in Appendix-A must be verified by iTech Labs.

11. Conclusion

While it is not possible to test all possible scenarios in a laboratory environment, iTech Labs has conducted a level of testing appropriate for a submission of this type.

Accordingly, subject to the above comment, iTech Labs certifies that the items under test comply with the relevant Technical Standards, unless otherwise stated.

Geoff Nicoll
Principal Consultant
iTech Labs Australia

13 January 2009

Kiren Sreekumar
Principal Consultant
iTech Labs Australia

13 January 2009



Appendix – A

1. Md5sum* of RNG source files

File Name	Size (bytes)	Md5sum
generator.c	8,606	916A3AACE43C8170640B02A9420D5F66
generator.h	3,536	A98A2B0D599D84A8AE5575BF8D0DE7A5
sha256.c	10,564	9A8F682809F30C957A73D5BC44780D32
sha256.h	2,020	C0647C23F402677FBB8C6E3EE0600554
client.c	4,175	D92F45A2B431C8E31003EEE6D8AC6809
client.h	2,143	FA14AE9E3B93146DD010DB3834726BED
libcards.c	1,603	943989A6A63908E117A56CBD2333FAF0
libcards.h	618	0D9B64B390000BF6BD96A03BDDE2D93F

* Md5sum is calculated using the Linux program md5sum.